بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای
سازمان فناوری اطلاعات ایران
معاونت امنیت فضای تولید و تبادل اطلاعات

پویش و ارائه راهکار کاهش مخاطرات درخصوص بهره‌برداری از آسیب‌پذیری‌های بحرانی اخیر سرورهای Microsoft Exchange

گزارش آسیب‌پذیری

شناسه سند ..... MaherReport_13991219-01
نوع سند ..... گزارش فنی
شماره نگارش ۰,۱
تاریخ نگارش ۱۳۹۹/۱۲/۱۹
طبقه‌بندی سند ..... **عادی**

تهران، خیابان شهید بهشتی، نرسیده به قائم مقام فراهانی، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ انتشار اسکریپت PowerShell توسط مایکروسافت

اخیراً مایکروسافت یک اسکریپت PowerShell را منتشر کرده است که مدیران شبکه و امنیت سازمان‌ها می‌توانند از آن برای بررسی آسیب‌پذیری‌های ProxyLogon استفاده کرده و سرور Microsoft Exchange خود را درخصوص نفوذ و بهره‌برداری از آسیب‌پذیری‌ها پویش کنند.

این اسکریپت در صفحه گیتهاب مایکروسافت با نام Test-ProxyLogon.ps1 منتشر شده است و عکس آن در زیر قرار داده شده است و آدرس صفحه گیتهاب آن به صورت زیر است.

https://github.com/microsoft/CSS-Exchange/tree/main/Security

286 lines (241 sloc) 11.8 KB Raw Blame

```powershell
# Checks for signs of exploit from CVE-2021-26855, 26858, 26857, and 27065.
#
# Examples
#
# Check the local Exchange server only and save the report:
# .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
#
# Check all Exchange servers and save the reports:
# Get-ExchangeServer | .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
#
# Check all Exchange servers, but only display the results, don't save them:
# Get-ExchangeServer | .\Test-ProxyLogon.ps1


[CmdletBinding()]
param (
    [Parameter(ValueFromPipeline = $true, ValueFromPipelineByPropertyName = $true)]
    [string[]]
    $ComputerName = $env:COMPUTERNAME,
```

مایکروسافت برای استفاده از این اسکریپت فرمان‌های مختلفی را برای پویش یک سرور و یا تمامی سرورهای Microsoft Exchange یک سازمان در نظر گرفته است. برای پویش تمامی سرورهای Microsoft Exchange یک سازمان و ذخیره لاگ‌های آن بر روی دسکتاپ دستور زیر در Exchange Management Shell اجرا شود:

```
Get-ExchangeServer | .\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
```

اگر خواهان پویش سرور محلی و ذخیره لاگ‌های آن هستید دستور زیر اجرا گردد:

```
.\Test-ProxyLogon.ps1 -OutPath $home\desktop\logs
```

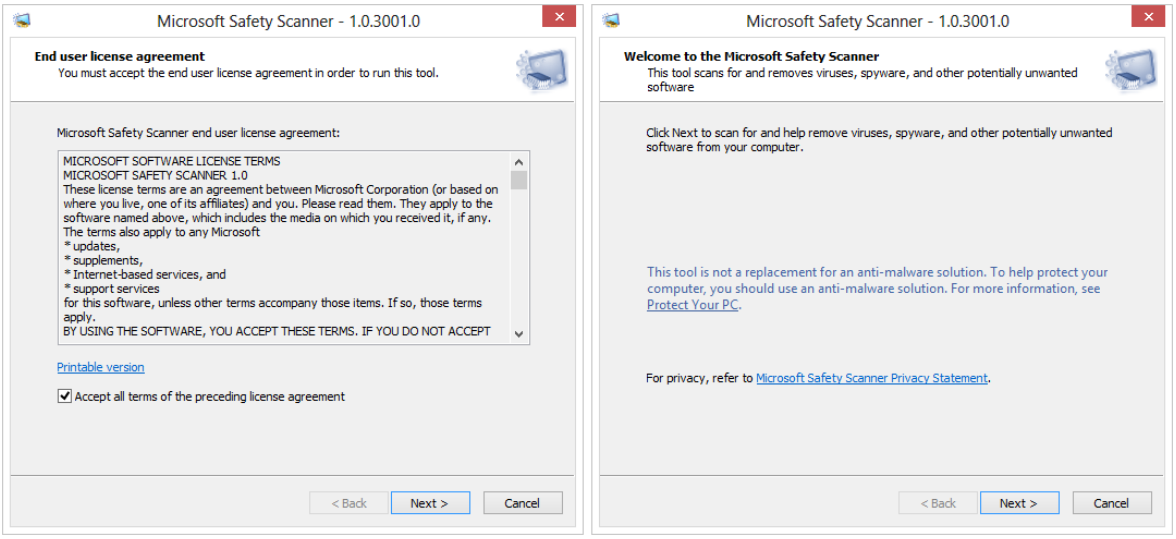
همچنین اگر صرفاً فقط خواهان پویش سرور محلی بدون ذخیره نتایج هستید، می‌توان دستور زیر اجرا شود:

```
.\Test-ProxyLogon.ps1
```

۲ استفاده از Microsoft Safety Scanner

یکی دیگر از راهکاری پویش سرور استفاده از ابزار Microsoft Safety Scanner است که برای نسخه‌های مختلف ویندوز و ویندوز سرور ارائه شده است و از طریق لینک زیر قابل دانلود می‌باشد.

https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download



این ابزار به صورت قابل‌حمل بوده و نیاز به نصب ندارد. برای پویش سرور مراحل زیر انجام شود:

- دانلود و اجرای ابزار
- انتخاب نوع پویش و زدن شروع پویش
- بررسی نتایج پویش در خلاصه خروجی نشان داده شده و برای بررسی دقیق نتایج رجوع به فایل لاگ در مسیر:

%SYSTEMROOT%\debug\msert.log

البته توصیه شده است که این ابزار جایگزینی برای Microsoft Defender نبوده و باید در سرور ویندوزی از هردوی آنها استفاده کرد. در به‌روزرسانی اخیر مایکروسافت نیز Microsoft Defender برای پویش این آسیب‌پذیری‌ها به‌روز شده و می‌توان از آن برای پویش سرور Microsoft Exchange برای این منظور استفاده کرد.

۳ اسکریپتی برای بررسی وب‌شل‌های آپلود شده پس از نفوذ

پس از انتشار اخبار مربوط به این آسیب‌پذیری‌ها و بهره‌برداری فعال و گسترده از آن‌ها، مراکز مختلف امنیتی راهکارها و اسکریپت‌های مختلفی برای پویش سرورها ارائه کردند. یکی از این اسکریپت‌ها برای بررسی وب‌شل‌های آپلود شده پس از نفوذ و بهره‌برداری است که از طریق آدرس زیر می‌توان آن را دریافت کرد:

https://github.com/cert-lv/exchange_webshell_detection

در این اسکریپت که توسط مرکز CERT کشور لتونی ارائه شده، پویشی برای وب‌شل‌های شناخته شده و معروف بر روی سرور انجام می‌شود. برای اجرای این اسکریپت کافی است دستور زیر اجرا شود:

```
detect_webshells.ps1
```

دستور بالا بهتر است در مسیرهای زیر که رایج‌تر بوده و توسط مهاجمین در اغلب موارد وب‌شل آپلود شده، اجرا شود:

```
inetpub/wwwroot/aspnet_client/
-----------------------------
$($env:exchangeinstallpath)/Frontend/
-----------------------------
```

۴ اسکریپت Exchange Server Health Checker

اسکریپت Exchange Server Health Checker نیز برای پویش پیکربندی‌های ناصحیح و ضعف‌های احتمالی در این روزها مورد توجه بوده است. لینک گیتهاب مربوط به این اسکریپت در زیر قرار داده شده است:

https://github.com/dpaulson45/HealthChecker

این اسکریپت نسخه‌های ۲۰۱۳، ۲۰۱۶ و ۲۰۱۹ از Microsoft Exchange را پشتیبانی می‌کند. اجرای این اسکریپت پاورشل برای پویش یک سرور محلی به صورت زیر خواهد بود:

```
.\HealthChecker.ps1
```

همچنین میتوان از طریق فرمان زیر نتایج را در قالب خروجی HTML دریافت کرد.

```
.\HealthChecker.ps1 -BuildHtmlServersReport
```

۵ راهکارهایی برای کاهش خطرات

باید توجه داشت که مهمترین راهکار انجام به‌روزرسانی منتشر شده از طرف مایکروسافت است تا وصله‌ها اعمال گردد. مایکروسافت و دیگر مراکز امنیتی برای کاهش خطرات ناشی از نفوذها و بهره‌برداری از این آسیب‌پذیری‌ها راهکارهای مختلفی را ارائه کرده‌اند که در ادامه این موارد بررسی می‌شوند.

- **پویش فایل‌های لاگ سرور Microsoft Exchange**

❖ برای شناسایی بهره‌برداری از آسیب‌پذیری با شناسه CVE-2021-26855 لاگ‌های Exchange HttpProxy بررسی شوند. این لاگ‌ها در مسیر زیر قرار دارند.

```
%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\HttpProxy
```

یک نمونه اسکریپت پاورشل برای بررسی لاگ به صورت زیر است:

```
Import-Csv -Path (Get-ChildItem -Recurse -Path
"$env:PROGRAMFILES\Microsoft\Exchange Server\V15\Logging\HttpProxy" -Filter
'*.log').FullName | Where-Object { $_.AuthenticatedUser -eq '' -and
($_.AnchorMailbox -like 'ServerInfo~*/*' -or $_.BackEndCookie -like
'Server~*/*~*')} | select DateTime, AnchorMailbox, UrlStem, RoutingHint,
ErrorCode, TargetServerVersion, BackEndCookie, GenericInfo, GenericErrors,
UrlHost, Protocol, Method, RoutingType, AuthenticationType, ServerHostName,
HttpStatus, BackEndStatus, UserAgent
```

❖ برای شناسایی بهره‌برداری از آسیب‌پذیری با شناسه CVE-2021-26858 لاگ‌های Exchange بررسی شوند. این لاگ‌ها در مسیر زیر قرار دارند.

```
C:\Program Files\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog
```

فایل‌های مربوط به بهره‌برداری در اغلب موارد در مسیر زیر دانلود شده‌اند:

```
%PROGRAMFILES%\Microsoft\Exchange Server\V15\ClientAccess\OAB\Temp
```

البته در برخی دیگر از بهره‌برداری‌ها، فایل‌ها در مسیرهای دیگری مانند UNC دانلود شده بودند. از دستور زیر برای جستجوی بهره‌برداری احتمالی می‌توان استفاده شود:

```
findstr /snip /c:"Download failed and temporary file"
"%PROGRAMFILES%\Microsoft\Exchange Server\V15\Logging\OABGeneratorLog\*.log"
```

❖ برای شناسایی بهره‌برداری از آسیب‌پذیری با شناسه CVE-2021-26857 لاگ‌های Windows Application event بررسی شوند. بهره‌برداری از این آسیب‌پذیری رویدادهای برنامه با مشخصات زیر را ایجاد می‌کند:

```
Source: MSExchange Unified Messaging
EntryType: Error
Event Message Contains: System.InvalidCastException
```

فرمان‌های پاورشل زیر پرس‌وجو در لاگ رویداد برنامه است که می‌تواند بسیار مفید باشد:

```
Get-EventLog -LogName Application -Source "MSExchange Unified Messaging" -
EntryType Error | Where-Object { $_.Message -like
"*System.InvalidCastException*" }
```

❖ برای شناسایی بهره‌برداری از آسیب‌پذیری با شناسه CVE-2021-27065 لاگ‌های Exchange بررسی شوند. این لاگ‌ها در مسیر زیر قرار دارند.

```
C:\Program Files\Microsoft\Exchange Server\V15\Logging\ECP\Server
```

تمامی موارد VirtualDirectory properties <AppName> نباید دارای هرگونه اسکریپتی باشند. همچنین InternalUrl و ExternalUrl فقط باید شامل URIهای معتبر باشند.

می‌توان از فرمان پاورشل زیر برای جستجوی بهره‌برداری احتمالی استفاده شود:

```
Select-String -Path "$env:PROGRAMFILES\Microsoft\Exchange
Server\V15\Logging\ECP\Server\*.log" -Pattern 'Set-.+VirtualDirectory'
```

- **هش‌های وب‌شل‌ها**

در زیر هش مربوط به وب‌شل‌های رایج استفاده شده، قرار گرفته است:

```
b75f163ca9b9240bf4b37ad92bc7556b40a17e27c2b8ed5c8991385fe07d17d0
097549cf7d0f76f0d99edf8b2d91c60977fd6a96e4b8c3c94b0b1733dc026d3e
2b6f1ebb2208e93ade4a6424555d6a8341fd6d9f60c25e44afe11008f5c1aad1
65149e036fff06026d80ac9ad4d156332822dc93142cf1a122b1841ec8de34b5
511df0e2df9bfa5521b588cc4bb5f8c5a321801b803394ebc493db1ef3c78fa1
4edc7770464a14f54d17f36dc9d0fe854f68b346b27b35a6f5839adf1f13f8ea
811157f9c7003ba8d17b45eb3cf09bef2cecd2701cedb675274949296a6a183d
1631a90eb5395c4e19c7dbcbf611bbe6444ff312eb7937e286e4637cb9e72944
```

همچنین مسیر مربوط به این وب‌شل‌ها در اغلب موارد به صورت زیر بوده‌اند:

```
C:\inetpub\wwwroot\aspnet_client\
C:\inetpub\wwwroot\aspnet_client\system_web\
%PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy\owa\auth\
C:\Exchange\FrontEnd\HttpProxy\owa\auth\
```

با تحلیل و بررسی گزارش‌های انجام شده مشخص شد که نام‌های مربوط به وب‌شل‌های که شناسایی شده‌اند نیز به صورت زیر می‌باشند:

```
web.aspx
help.aspx
document.aspx
errorEE.aspx
errorEEE.aspx
errorEW.aspx
errorFF.aspx
healthcheck.aspx
aspnet_www.aspx
aspnet_client.aspx
xx.aspx
shell.aspx
aspnet_iisstart.aspx
one.aspx
```

در نهایت در صورت وجود شواهد نفوذ و درخواست امداد با آدرس ایمیل report@cert.ir مکاتبه کنید.

۶ منابع

- https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- https://www.bleepingcomputer.com/news/microsoft/this-new-microsoft-tool-checks-exchange-servers-for-proxylogon-hacks/
- https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
- https://www.zdnet.com/article/check-to-see-if-youre-vulnerable-to-microsoft-exchange-server-zero-days-using-this-tool/
- https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
- https://github.com/microsoft/CSS-Exchange/tree/main/Security
- https://github.com/cert-lv/exchange_webshell_detection
- https://github.com/dpaulson45/HealthChecker